WHAT IS CLAIMED IS:

1. A method of secure session management for a web farm, the web farm including a first server and a second server, the second server having a requested web page, the method comprising the steps of:

receiving, at the first server, a request for the requested web page from a browser, said request including an encrypted session token;

decrypting said encrypted session token at the first server to obtain a session token;

redirecting said request to the second server, including transmitting said session token to the second server; and

verifying said session token.

2. The method claimed in claim 1, further including steps of creating a new session token, encrypting said new session token at the second server to produce a new encrypted session token, and transmitting a response to said browser from the second server, wherein said response includes said new encrypted session token.

3. The method claimed in claim 2, wherein said session token includes a session ID and a timestamp, and wherein said step of creating a new session token includes generating a new session ID and updating said timestamp.

4. The method claimed in claim 2, further including a step of updating a common session database by replacing said session token with said new session token in said common session database.

5. The method claimed in claim 1, wherein said session token includes a session ID and a timestamp.

6. The method claimed in claim 5, wherein a common session database contains a stored session ID and a stored timestamp, and wherein said step of verifying includes comparing said session ID and said timestamp with said stored session ID and said stored timestamp.

7. The method claimed in claim 5, further including a step of determining whether a session has timed out, said step of determining including determining an elapsed time between said timestamp and a current server time, and comparing said elapsed time with a predetermined maximum time to determine whether said session has timed out.

8. The method claimed in claim 7, including a step of closing said session if said session has timed out.

9. The method claimed in claim 1, wherein said step of transmitting includes incorporating said session token into a URL.

10. The method claimed in claim 1, wherein a session management web service performs said step of verifying, said session management web service being accessible to said first server and said second server, and wherein said step of verifying includes comparing said session token with stored session data.

11. The method claimed in claim 10, wherein the web farm further includes a common session database containing said stored session data.

12. The method claimed in claim 1, wherein said requested web page includes a web resource selected

from the group including an applet, an HTML page, a Java server page, and an Active server page.

13. A system for secure session management, the system being coupled to a network and receiving a request for a requested web page from a browser via the network, the request including an encrypted session token, the system comprising:

a first server including a first request handler for receiving the request and decrypting the encrypted session token to produce a session token;

a second server including the requested web page;

a common session database including stored session data; and

a session management web service, accessible to said first server and said second server and including a validation component for comparing said session token with said stored session data;

wherein said first request handler redirects the request to said second server and transmits the session token to said second server.

14. The system claimed in claim 13, wherein said session management web service includes a token generator for creating a new session token for said second server, and wherein said second server includes a second request handler, said second request handler encrypting said new session token to produce a new encrypted session token and transmitting a response to said browser, wherein said response includes said new encrypted session token.

15. The system claimed in claim 14, wherein said session token includes a session ID and a timestamp, and wherein said token generator generates a new session

ID, and updates said timestamp based upon a current server time.

16. The system claimed in claim 14, wherein said session management web service replaces said session token within said common session database with said new session token.

17. The system claimed in claim 13, wherein said session token includes a session ID and a timestamp.

18. The system claimed in claim 17, wherein said stored session data includes a stored session ID and a stored timestamp, and wherein said validation component compares said session ID and said timestamp with said stored session ID and said stored timestamp.

19. The system claimed in claim 17, wherein said validation component further determines an elapsed time between said timestamp and a current server time, and compares said elapsed time with a predetermined maximum time to determine whether a session has timed out.

20. The system claimed in claim 19, wherein said session management web service closes said session if said validation component indicates said session has timed out.

21. The system claimed in claim 13, wherein said first request handler incorporates said session token into a URL in order to transmit said session token to said second server.

22. The system claimed in claim 13, wherein the requested web page includes a web resource selected from the group including an applet, an HTML page, a Java server page, and an Active server page.

23. A computer program product having a computer-readable medium tangibly embodying computer executable instructions for secure session management for a web farm, the web farm including a first server and a second server, the second server having a requested web page, the computer executable instructions including of:

computer executable instructions for receiving, at the first server, a request for the requested web page from a browser, said request including an encrypted session token;

computer executable instructions for decrypting said encrypted session token at the first server to obtain a session token;

computer executable instructions for redirecting said request to the second server, including computer executable instructions for transmitting said session token to the second server; and

computer executable instructions for verifying said session token.

24. The computer program product claimed in claim 23, further including computer executable instructions for creating a new session token, encrypting said new session token at the second server to produce a new encrypted session token, and transmitting a response to said browser from the second server, wherein said response includes said new encrypted session token.

25. The computer program product claimed in claim 24, wherein said session token includes a session ID and a timestamp, and wherein said computer executable instructions for creating a new session token

include computer executable instructions for generating a new session ID and updating said timestamp.

26. The computer program product claimed in claim 24, further including computer executable instructions for updating a common session database by replacing said session token with said new session token in said common session database.

27. The computer program product claimed in claim 23, wherein said session token includes a session ID and a timestamp.

28. The computer program product claimed in claim 27, wherein a common session database contains a stored session ID and a stored timestamp, and wherein said computer executable instructions for verifying include computer executable instructions for comparing said session ID and said timestamp with said stored session ID and said stored timestamp.

29. The computer program product claimed in claim 27, further including computer executable instructions for determining whether a session has timed out, said computer executable instructions for determining including computer executable instructions for determining an elapsed time between said timestamp and a current server time, and comparing said elapsed time with a predetermined maximum time to determine whether said session has timed out.

30. The computer program product claimed in claim 29, including computer executable instructions for closing said session if said session has timed out.

31. The computer program product claimed in claim 23,

wherein said computer executable instructions for transmitting include computer executable instructions for incorporating said session token into a URL.

32. The computer program product claimed in claim 23, wherein said computer executable instructions for verifying comprise a session management web service, said session management web service being accessible to said first server and said second server, and wherein said computer executable instructions for verifying include computer executable instructions for comparing said session token with stored session data.

33. The computer program product claimed in claim 32, wherein the web farm further includes a common session database containing said stored session data.

34. The computer program product claimed in claim 23, wherein said requested web page includes a web resource selected from the group including an applet, an HTML page, a Java server page, and an Active server page.